

GAU 2185 #2



I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the date indicated below.

Janice E. Favreau

Name of Person Mailing Paper or Fee

4/3/01
Date of Signature

RECEIVED

APR 11 2001

Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of)

Shigeaki Yamane et al.)

for PORTABLE RECORDING MEDIUM)

AND METHOD OF USING)

PORTABLE RECORDING MEDIUM)

Serial No: 09/781,839)

Filed On: February 12, 2001)

Group Art Unit: 2185

Our Docket No: 6609-01

Hartford, Connecticut, April 3, 2001

Assistant Commissioner
for Patents
Washington, D. C. 20231

SUBMISSION OF CERTIFIED COPY
UNDER 35 USC §119 AND 37 CFR §1.55(a)

S I R:

Submitted herewith is a certified copy of Japanese Patent Application No. 2000-036399 which was filed on February 15, 2000, in accordance with 35 USC §119 and 37 CFR §1.55(a) to form a part of the above-identified application as filed.

Respectfully submitted,

By

John C. Linderman
Registration No. 24,420
Attorney for Applicant

McCormick, Paulding & Huber LLP
CityPlace II
185 Asylum Street
Hartford, Connecticut 06103-4102



日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 2月15日

出願番号

Application Number:

特願2000-036399

出願人

Applicant(s):

ベーステクノロジー株式会社

RECEIVED

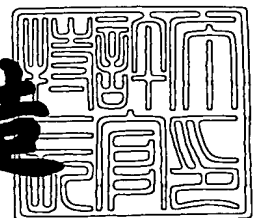
APR 11 2001

Technology Center 2100

2001年 2月 2日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3003821

【書類名】 特許願

【整理番号】 P-3648

【提出日】 平成12年 2月15日

【あて先】 特許庁長官殿

【国際特許分類】 A61B 5/177

【発明者】

【住所又は居所】 東京都新宿区西新宿 7 - 2 2 - 4 5 ベーステクノロジー
一株式会社内

【氏名】 山根 茂昭

【発明者】

【住所又は居所】 東京都新宿区西新宿 7 - 2 2 - 4 5 ベーステクノロジー
一株式会社内

【氏名】 今城 忠浩

【発明者】

【住所又は居所】 東京都新宿区西新宿 7 - 2 2 - 4 5 ベーステクノロジー
一株式会社内

【氏名】 吉田 直邦

【特許出願人】

【識別番号】 397065952

【氏名又は名称】 ベーステクノロジー株式会社

【代理人】

【識別番号】 100080001

【弁理士】

【氏名又は名称】 筒井 大和

【電話番号】 03-3366-0787

【選任した代理人】

【識別番号】 100093023

【弁理士】

【氏名又は名称】 小塚 善高

【選任した代理人】

【識別番号】 100102853

【弁理士】

【氏名又は名称】 鷹野 寧

【手数料の表示】

【予納台帳番号】 006909

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 可搬性記録媒体および可搬性記録媒体の使用方法

【特許請求の範囲】

【請求項 1】 アプリケーションソフトウェアと、前記アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者による前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されていることを特徴とする可搬性記録媒体。

【請求項 2】 請求項 1 記載の可搬性記録媒体において、前記アプリケーションソフトウェアおよび前記認証ソフトウェアは、前記可搬性記録媒体の読み出し専用領域に格納され、前記個人識別情報は、前記可搬性記録媒体の書き換え可能領域に暗号化されて格納されていることを特徴とする可搬性記録媒体。

【請求項 3】 請求項 1 または 2 記載の可搬性記録媒体において、前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第 1 の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに依頼し、前記認証サーバーから照合結果を受け取ることで前記個人認証を行う第 2 の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体。

【請求項 4】 請求項 1, 2 または 3 記載の可搬性記録媒体において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体。

【請求項 5】 アプリケーションソフトウェアが格納された可搬性記録媒体に、前記アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による前記可搬性記録媒体の前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行うことで、正当な前記利用者に、前記可搬性記録媒体に格納されている前記アプリケーションソフトウェアを使用させることを特徴とする可搬性記録媒体の使用方法。

【請求項 6】 請求項 5 記載の可搬性記録媒体の使用方法において、前記ア

アプリケーションソフトウェアとともに前記可搬性記録媒体に格納されている認証ソフトウェアを用いて前記個人認証を行うことを特徴とする可搬性記録媒体の使用方法。

【請求項 7】 請求項 6 記載の可搬性記録媒体の使用方法において、前記アプリケーションソフトウェアとともに前記可搬性記録媒体に格納されている前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第 1 の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに依頼し、前記認証サーバーから照合結果を受け取ることで前記個人認証を行う第 2 の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体の使用方法。

【請求項 8】 請求項 7 記載の可搬性記録媒体の使用方法において、前記認証サーバーは、複数の前記個人識別情報の各々と、個々の前記アプリケーションソフトウェアのライセンスキーとが対応付けて格納されたライセンスデータベースを持ち、前記個人識別情報に対応した前記ライセンスキーを前記照合結果として前記認証ソフトウェアの前記第 2 の認証機能に応答することで、前記可搬性記録媒体に格納された前記アプリケーションソフトウェアの利用機能の制限を行うことを特徴とする可搬性記録媒体の使用方法。

【請求項 9】 請求項 5， 6， 7 または 8 記載の可搬性記録媒体の使用方法において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体の使用方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、可搬性記録媒体およびその使用技術に関し、特に、高度かつ多様なセキュリティ管理を必要とするアプリケーションソフトウェアが格納された可搬性記録媒体等に適用して有効な技術に関する。

【0002】

【従来の技術】

たとえば、いわゆるインターネット等の情報ネットワークの発達および高性能のパーソナルコンピュータの広範な普及に伴い、パーソナルコンピュータを取引端末とする、電子商取引や、証券、金融サービスが普及してきている。

【0003】

このようなパーソナルコンピュータを取引端末とする上述の各種サービスは、特定のパーソナルコンピュータに備えられた固定ディスク装置（HDD）等の外部記憶装置に当該サービス専用の端末ソフトウェア（アプリケーションソフトウェア）を実装して行われることが多い。

【0004】

【発明が解決しようとする課題】

ところで、特定のパーソナルコンピュータに端末ソフトウェアを実装して利用する場合には、当該サービスの利用場所が特定のパーソナルコンピュータの設置場所に制約され、利用者にとって利便性に欠ける、という技術的課題がある。

【0005】

さらに、実際のサービス利用に先立って、パーソナルコンピュータへのソフトウェアのインストール作業が必須となり、パーソナルコンピュータの知識に乏しい一般の利用者にとってはサービス利用の敷居が高くなり、サービス普及の障害となるとともに利便性にも欠ける。

【0006】

一方、最近では、CD-RW（Compact Disc-Rewritable）、MO（Magneto Optical disc）、DVD（Digital Versatile Disc）等に代表される書き換え可能な可搬性の大容量記憶媒体が利用可能になってきている。特に、CD-RWは、媒体価格およびドライブ価格ともに安価で、かつ前世代のCD-ROMも利用可能なことから急速に普及している。

【0007】

そこで、このCD-RW等の大容量可搬媒体に各種サービスに専用の端末ソフトウェアを纏めて実装しておき、任意のパーソナルコンピュータに装填されたCD-RW上から直接に任意の端末ソフトウェアを立ち上げることで、パーソナル

コンピュータの設置場所に制約されないポータビリティの高いサービスを実現することが考えられる。

【 0 0 0 8 】

ところが、大容量可搬媒体は、ポータビリティが高いが故に、紛失、盗難等のリスクが常に付きまとい、通常のパスワードによる管理では、本人確認等のセキュリティ管理が不十分となる。このため、電子商取引や、証券、金融サービス等のように高いセキュリティを要求されるサービスには適用が躊躇される。

【 0 0 0 9 】

このセキュリティ対策として、たとえば、利用者に複雑なパスワードを設定させることが考えられるが、パスワードの暗唱や秘匿等、利用者のパスワード管理負担が大きくなる、という別の技術的課題を生じる。

【 0 0 1 0 】

本発明の目的は、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【 0 0 1 1 】

本発明の他の目的は、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【 0 0 1 2 】

本発明の他の目的は、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【 0 0 1 3 】

【課題を解決するための手段】

本発明は、アプリケーションソフトウェアが格納される可搬性記録媒体に、指紋等の個人識別情報を予め登録しておき、この個人識別情報を用いた個人認証により、真正のユーザーのみにアプリケーションソフトウェアの利用を可能ならし

るものである。

【 0 0 1 4 】

すなわち、本発明の可搬性記録媒体は、アプリケーションソフトウェアと、アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者によるアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されるようにしたものである。

【 0 0 1 5 】

また、本発明の可搬性記録媒体の使用方法は、アプリケーションソフトウェアが格納された可搬性記録媒体に、アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による可搬性記録媒体のアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行うことで、正当な利用者に、可搬性記録媒体に格納されているアプリケーションソフトウェアを使用させるものである。

【 0 0 1 6 】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【 0 0 1 7 】

(実施の形態 1)

図 1 は、本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図であり、図 2 および図 3 は、本実施の形態の可搬性記録媒体の使用方の一例を示すフローチャートである。

【 0 0 1 8 】

本実施の形態では、可搬性記録媒体の一例として、CD-RW を例に採って説明する。

【 0 0 1 9 】

本実施の形態の CD-RW 1 0 0 0 は、データの記憶領域が、読み出し専用の物理アクセスプロテクトエリア 1 0 0 1 と、書き換え可能なリライタブルエリア 1 0 0 2 にて構成されている。

【 0 0 2 0 】

物理アクセスプロテクトエリア1001は、後述の各種ソフトウェアの書き込み時に、書き換え不能なデータ書き込み方式を用いてデータ書き込みが実行されており、物理的に、書き換え等による改竄が不可能になっている。

【0021】

リライタブルエリア1002は、ソフトウェアによる暗号化にて書き込みデータの保護が行われるプロテクトエリア1002-1と、ユーザーや後述のアプリケーションプログラムが自由にアクセス可能なフリーエリア1002-2からなる。

【0022】

物理アクセスプロテクトエリア1001には、ユーザー認証プログラム10、指紋認証エンジン20、2フェーズ認証プログラム30、トレーサー40、アプリケーション管理プログラム50、複数のアプリケーションソフトウェア50A、等が格納されている。

【0023】

ユーザー認証プログラム10は、後述のように、外部から入力されるユーザーの指紋情報と、予め登録されている指紋情報とに基づいて真正のユーザーを判別する処理を行うソフトウェアであり、ユーザーID管理機能10-1、指紋情報管理機能10-2、認証要求機能10-3等の機能を備えている。

【0024】

指紋認証エンジン20は、ユーザー認証プログラム10の配下で指紋情報の照合処理を行うソフトウェアであり、入力された指紋情報および登録されている指紋情報から各々の特徴情報を抽出する指紋データ抽出機能20-1、および特徴情報の照合による一致／不一致の判定を行う指紋照合機能20-2等の機能を備えている。

【0025】

2フェーズ認証プログラム30は、後述のような外部の認証サーバーに指紋照合を依頼する等の認証処理を行うソフトウェアであり、認証サーバー連携機能30-1等を備えている。

【0026】

トレーサー 4 0 は、指紋による認証プロセスの監視や記録等の処理を行うものであり、後に不正アクセスの解析等を行うべく、たとえば認証が不成功に終わったときに入力された指紋情報等を記録する指紋データ収集機能 4 0 - 1 等を備えている。

【 0 0 2 7 】

アプリケーション管理プログラム 5 0 は、後述の 2 フェーズ認証プログラム 3 0 にて認証サーバー等から得られるライセンスキー等に応じて、各種のアプリケーションソフトウェア 5 0 A の各々について、利用可能な機能等の制限を行うためのアプリケーションライセンスキー管理機能 5 0 - 1 等を備えている。

【 0 0 2 8 】

アプリケーションソフトウェア 5 0 A としては、たとえば、銀行との決済系取引関連のサービスをサポートするバンキング・トランザクションソフトウェア、投資信託、株式、その他の金融商品の運用管理サービスを行うアセット・マネジメントソフトウェア、保険商品サービスを行うライフ・プランニングソフトウェア、投資関連情報、企業情報、等を提供するファイナンシャル・インフォメーションソフトウェア、電子商取引を行うための電子商取引ソフトウェア、等を格納することができる。

【 0 0 2 9 】

リライタブルエリア 1 0 0 2 のプロテクトエリア 1 0 0 2 - 1 には、ユーザー情報 6 0、指紋情報 7 0、ログ情報 8 0、認証キー情報 9 0、等が格納される。

【 0 0 3 0 】

ユーザー情報 6 0 は、個々のユーザーにユニークに付与されたユーザー ID 6 0 - 1、指紋登録有無フラグ 6 0 - 2、等の情報からなる。

【 0 0 3 1 】

指紋情報 7 0 は、後述の登録処理にて得られたユーザー ID 7 0 - 1、および指紋データ 7 0 - 2、等の情報からなる。

【 0 0 3 2 】

ログ情報 8 0 は、指紋認証処理で照合が不成功に終わったときに得られたユーザー ID 8 0 - 1、および指紋データ 8 0 - 2、図示しない日時データ等の情報

からなる。

【0033】

認証キー情報90は、ユーザーID90-1、アプリケーションソフトウェア名90-2、ライセンスキー90-3、等の情報からなる。

【0034】

図6は、本実施の形態の可搬性記録媒体の利用方法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【0035】

図6のパーソナルコンピュータ2000において、2001はマイクロプロセッサ(MPU)、2002はマイクロプロセッサ2001にて実行されるソフトウェアやデータ等が格納される主記憶、2003は、固定ディスク装置(HDD)等の外部記憶装置、2004は、外部から装填されるCD-RW1000に対するデータの入出力を行うCD-ROMドライブ、CD-RWドライブ等の可搬媒体ドライブ、2005はインターネット等の情報ネットワークに接続されるネットワークインタフェース、2006はユーザーインタフェース、2007は指紋等の個人識別情報を取り込むための個人識別情報入力装置、2008は、これらの各部が接続されるバスである。

【0036】

個人識別情報入力装置2007は、たとえば、ユーザーインタフェース2006を構成するディスプレイ、キーボード、マウス等と一体型の装置でもよい、これらとは独立な装置形態であってもよい。

【0037】

主記憶2002には、たとえば、パーソナルコンピュータ用の汎用オペレーティングシステム2002aが常駐し、この汎用オペレーティングシステム2002aの上で、CD-RW1000から当該主記憶2002にロードされる、上述の、アプリケーションソフトウェア50Aが稼働する。

【0038】

以下、本実施の形態の可搬性記録媒体およびその使用方法の作用の一例について説明する。なお、図2において括弧付きで記載されている符号は、当該処理を

実行するプログラムや機能の符号を示している。

【 0 0 3 9 】

まず、図 2 のフローチャート等を参照して、正当なユーザーの指紋情報の CD-RW 1 0 0 0 への登録処理について説明する。なお、この登録処理は、たとえば、アプリケーションソフトウェア 5 0 A 等を CD-RW 1 0 0 0 に格納してユーザーに提供する際に、提供者の管理下で正当なユーザーに登録処理を行わせることで、セキュリティが保たれる。

【 0 0 4 0 】

CD-RW 1 0 0 0 のユーザーは、当該 CD-RW 1 0 0 0 を可搬媒体ドライブ 2 0 0 4 に装填することにより、OS 2 0 0 2 a の媒体自動起動メカニズムにて CD-RW 1 0 0 0 を起動し、ユーザー認証プログラム 1 0、指紋認証エンジン 2 0 等を主記憶 2 0 0 2 にロードして実行する（ステップ S 0 0 1）。

【 0 0 4 1 】

なお、CD-RW 1 0 0 0 の起動は、OS 2 0 0 2 a の媒体自動起動メカニズムを用いて行わせることに限らず、メニュープログラムを立ち上げて、当該メニュープログラムから行わせるようにしてもよい。

【 0 0 4 2 】

ユーザー認証プログラム 1 0 のユーザー ID 管理機能 1 0 - 1 は、ユーザー情報 6 0 の指紋登録有無フラグ 6 0 - 2 を参照して、登録済か否かを判定し（ステップ S 0 0 2）、登録済でない場合は、指紋登録を促す認証情報設定画面をユーザーに提示する（ステップ S 0 0 3）。

【 0 0 4 3 】

この画面を見たユーザーは、まず、所定の形式のユーザー ID を入力し（ステップ S 0 0 4）、入力された当該ユーザー ID は、ユーザー ID 管理機能 1 0 - 1 により、ユーザー情報 6 0 にユーザー ID 6 0 - 1 として書き込まれる（ステップ S 0 0 5）。

【 0 0 4 4 】

次に、ユーザーは自己の指紋を個人識別情報入力装置 2 0 0 7 にて読み取らせ（ステップ S 0 0 6）、読み取られた指紋情報は、ユーザー認証プログラム 1 0

にて起動された指紋認証エンジン 2 0 の指紋データ抽出機能 2 0 - 1 にて特徴情報が指紋データとして抽出され（ステップ S 0 0 7）、抽出された指紋データは、指紋情報管理機能 1 0 - 2 による暗号化を経て、ユーザー I D とともに、ユーザー I D 7 0 - 1 および指紋データ 7 0 - 2 として指紋情報 7 0 に格納され（ステップ S 0 0 8）、指紋データ登録処理が完了する。

【 0 0 4 5 】

次に、上述のような登録後における任意の契機でのアプリケーションソフトウェアの利用方法の一例について説明する。

【 0 0 4 6 】

C D - R W 1 0 0 0 のユーザーは、当該 C D - R W 1 0 0 0 を、最寄りのパーソナルコンピュータ 2 0 0 0 の可搬媒体ドライブ 2 0 0 4 に装填することにより、O S 2 0 0 2 a の媒体自動起動メカニズムにて C D - R W 1 0 0 0 を起動し、ユーザー認証プログラム 1 0、指紋認証エンジン 2 0 等を主記憶 2 0 0 2 にロードして実行する（ステップ S 0 1 0）。

【 0 0 4 7 】

ユーザー認証プログラム 1 0 のユーザー I D 管理機能 1 0 - 1 は、ユーザー情報 6 0 の指紋登録有無フラグ 6 0 - 2 を参照して、登録済を確認し（ステップ S 0 1 1）、正当なユーザーか否かを判別するための指紋認証を行うべく、ユーザーに指紋読み取り処理の実行を促す指紋認証画面をユーザーに提示する（ステップ S 0 1 2）。

【 0 0 4 8 】

この画面を見たユーザーは、個人識別情報入力装置 2 0 0 7 から自己の指紋を入力し（ステップ S 0 1 3）、読み取られた指紋から、指紋認証エンジン 2 0 の指紋データ抽出機能 2 0 - 1 にて特徴情報が指紋データとして抽出され、同時に指紋データ抽出機能 2 0 - 1 は、指紋情報 7 0 から登録されている指紋データ 7 0 - 2 を読み出し（ステップ S 0 1 4）、指紋照合機能 2 0 - 2 にて、入力された指紋データと登録済の指紋データ 7 0 - 2 の一致／不一致の照合判定を行い（ステップ S 0 1 5）、一致すると判定された場合には、ユーザーからの任意のアプリケーションソフトウェア 5 0 A の起動要求を受け付け、利用を許可して（ス

テップ S 0 1 6)、当該アプリケーションソフトウェア 5 0 A を、C D - R W 1 0 0 0 から読み出して起動し、ユーザーに利用させる(ステップ S 0 1 7)。

【 0 0 4 9 】

起動されたアプリケーションソフトウェア 5 0 A は、稼働に必要なデータおよび稼働中に発生したデータの中でセキュリティ管理必要なデータは、C D - R W 1 0 0 0 のプロテクトエリア 1 0 0 2 - 1 の空き領域を利用して暗号化して書き込み、その他のデータは、フリーエリア 1 0 0 2 - 2 を利用して記録する。これにより、C D - R W 1 0 0 0 のみで稼働する。

【 0 0 5 0 】

なお、上述のように単に、アプリケーションソフトウェア 5 0 A を起動して利用させるだけに限らず、たとえば、ユーザー情報 6 0 あるいは指紋情報 7 0 の一部に、任意のアプリケーションソフトウェア 5 0 A と、ユーザー I D にて特定される特定ユーザー毎のライセンスレベル情報を設定しておき、ステップ S 0 1 6 の起動時に、当該アプリケーションソフトウェア 5 0 A にて利用可能な機能に制限を加えることもできる。

【 0 0 5 1 】

ステップ S 0 1 5 で不一致と判定された場合には、入力された指紋データやユーザー I D、日時データ等の経過情報をログ情報 8 0 に記録する(ステップ S 0 1 8)。このログ情報 8 0 を参照することで、当該 C D - R W 1 0 0 0 の利用経過や、不正使用の追跡、解析等を的確に行うことが可能になる。

【 0 0 5 2 】

なお、上述の判定処理では、ステップ S 0 1 3 ~ ステップ S 0 1 5、ステップ S 0 1 8 を所定の設定回数だけ反復させ、設定回数を超過した場合には、以降の当該 C D - R W 1 0 0 0 の使用を不能にする処理を加えてもよい。

【 0 0 5 3 】

このように、本実施の形態の C D - R W 1 0 0 0 およびその使用方法によれば、C D - R W 1 0 0 0 に予め登録された指紋等の個人識別情報を用いてユーザー認証を行うので、パスワード管理等の負担をユーザーにかけることなく、高い本人同一性の保証が可能となり、高いセキュリティを実現できる。また、可搬媒体

であるCD-RW1000にサービス提供に必要なすべてのアプリケーションソフトウェア50Aが格納されているので、CD-RW1000の利点である高いポータビリティと合わせて、CD-RW1000に格納されている多様なアプリケーションソフトウェア50Aの簡便な利用を可能にする効果がある。

【0054】

すなわち、CD-RW1000を携行するユーザーは、最寄りのパーソナルコンピュータ2000にCD-RW1000を装填するだけで、高いセキュリティを必要とする任意のサービスを受けることができる。

【0055】

この結果、電子商取引や金融関係等、高いセキュリティを必要とするアプリケーションソフトウェア50Aの格納および利用に、CD-RW1000を安心して利用でき、高いセキュリティおよびポータビリティによるユーザーおよびサービス提供側の利便性の向上を実現できる。

【0056】

(実施の形態2)

次に、本発明の可搬性記録媒体の使用方法的他の実施の形態について説明する。

【0057】

上述の実施の形態1の説明では、CD-RW1000に格納されていたユーザー認証プログラム100等を用いて、当該CD-RW1000にて閉じた状態で認証処理を行う例を説明したが、指紋の照合や認証処理を外部のサーバー等に依頼することで、より多様なアプリケーションソフトウェア50Aの使用における認証管理等を実現することもできる。以下のこのようなCD-RW1000の使用方法的一例について説明する。

【0058】

図4は、本発明の実施の形態2である可搬性記録媒体の使用方法的一例を示すフローチャートであり、図5は、本実施の形態2にて用いられる認証サーバーの構成の一例を示す概念図である。

【0059】

なお、実施の形態 1 と同一の構成要素については同一符号で引用することとし、重複する説明は割愛する。

【 0 0 6 0 】

まず、図 5 にて本実施の形態 2 における認証サーバー 3 0 0 0 の構成例について説明する。認証サーバー 3 0 0 0 は、制御ソフトウェア 3 0 0 1 として、ユーザー認証プログラム 1 0 0、指紋認証エンジン 2 0 0、トレーサー 3 0 0、アプリケーション利用管理プログラム 4 0 0、を備えている。

【 0 0 6 1 】

ユーザー認証プログラム 1 0 0 は、ユーザー ID 管理機能 1 0 0 - 1 を備えている。

【 0 0 6 2 】

指紋認証エンジン 2 0 0 は、指紋照合機能 2 0 0 - 1 を備えている。

【 0 0 6 3 】

トレーサー 3 0 0 は、指紋データ収集機能 3 0 0 - 1 を備えている。

【 0 0 6 4 】

アプリケーション利用管理プログラム 4 0 0 は、アプリケーション利用可否判定機能 4 0 0 - 1、アプリケーション利用ライセンスキー発行管理機能 4 0 0 - 2 を備えている。

【 0 0 6 5 】

また、認証サーバー 3 0 0 0 は、データベース 3 0 0 2 として、ユーザー情報 5 0 0、ログ情報 6 0 0、アプリケーション利用情報 7 0 0、等を備えている。

【 0 0 6 6 】

ユーザー情報 5 0 0 には、認証サーバー 3 0 0 0 の管理者にて登録管理されるユーザー ID 5 0 0 - 1 が記録されている。

【 0 0 6 7 】

ログ情報 6 0 0 には、指紋認証に失敗した認証処理にて得られたユーザー ID 6 0 0 - 1、および指紋データ 6 0 0 - 2、図示しない日時データ等が記録される。

【 0 0 6 8 】

アプリケーション利用情報 7 0 0 には、認証サーバー 3 0 0 0 の管理者にて登録管理される複数のユーザー ID 7 0 0 - 1 と、当該ユーザー ID 7 0 0 - 1 に対応して利用許可が設定されたアプリケーションソフトウェア 5 0 A のアプリケーションソフトウェア名 7 0 0 - 2、当該アプリケーションソフトウェア 5 0 A について当該ユーザー ID 7 0 0 - 1 のユーザーに許可設定された利用の可否や利用レベル等を示すライセンスキー 7 0 0 - 3 等が互いに対応付けられて格納されている。

【 0 0 6 9 】

以下、図 4 のフローチャートにて、本実施の形態 2 の作用の一例について説明する。なお、図 4 において括弧付きで記載されている符号は、当該処理を実行するプログラムや機能の符号を示している。

【 0 0 7 0 】

CD-RW 1 0 0 0 の起動は、上述の実施の形態 1 の場合と同様であるが、この実施の形態 2 の場合には、ユーザー認証プログラム 1 0 および 2 フェーズ認証プログラム 3 0 が使用される。そして、サービス選択の図示しないメニュープログラムが起動され、実際の各サービスの入口で、ユーザー認証プログラム 1 0 および 2 フェーズ認証プログラム 3 0 にて、認証サーバー 3 0 0 0 を利用した指紋認証を行う。

【 0 0 7 1 】

すなわち、まず、CD-RW 1 0 0 0 の起動時の任意のアプリケーションソフトウェア 5 0 A を用いるサービスを選択すると、ユーザー認証プログラム 1 0 によるユーザーからのユーザー ID および指紋の入力処理が実行され（ステップ S 0 2 0）、ユーザーから入力された指紋データおよび、図 2 のフローチャートの処理にて予め CD-RW 1 0 0 0 に登録されている登録済のユーザー ID 7 0 - 1、指紋データ 7 0 - 2、当該サービスにて起動されるアプリケーションソフトウェア 5 0 A の名前であるアプリケーションソフトウェア名 9 0 - 2 が、2 フェーズ認証プログラム 3 0 の認証サーバー連携機能 3 0 - 1 にて、認証サーバー 3 0 0 0 に送られる（ステップ S 0 2 1）。

【 0 0 7 2 】

これを受けた認証サーバー 3 0 0 0 は、ユーザー認証プログラム 1 0 0 にて、ユーザー ID 5 0 0 - 1 とユーザー ID 7 0 - 1 との照合によるユーザー確認を行った後（ステップ S 0 2 2）、ユーザーから入力された指紋データと、登録済の指紋データ 7 0 - 2 との照合を行う（ステップ S 0 2 3）。

【 0 0 7 3 】

そして、指紋照合結果が一致しない場合には、ユーザー（パーソナルコンピュータ 2 0 0 0）側から受信した指紋データ等をログ情報 6 0 0 に、日時データ等とともに記録するとともに（ステップ S 0 2 4）、当該サービスの利用不可をユーザーに応答する（ステップ S 0 2 5）。

【 0 0 7 4 】

指紋照合結果が一致した場合には、ユーザー側から受信したアプリケーションソフトウェア名 9 0 - 2 およびユーザー ID 7 0 - 1 をキーとしてアプリケーション利用情報 7 0 0 を参照することで、当該ユーザーによる当該アプリケーションソフトウェア 5 0 A の利用の可否を判定し（ステップ S 0 2 6）、アプリケーション利用情報 7 0 0 に未登録の場合には、利用不可をユーザー側に応答する（ステップ S 0 2 7）。

【 0 0 7 5 】

アプリケーション利用情報 7 0 0 に登録済の場合は、対応するライセンスキー 7 0 0 - 3 をアプリケーション利用情報 7 0 0 から読み出し（ステップ S 0 2 8）、ユーザー側のアプリケーションライセンスキー管理機能 5 0 - 1 に送信する（ステップ S 0 2 9）。

【 0 0 7 6 】

ユーザー側のアプリケーションライセンスキー管理機能 5 0 - 1 は、当該ライセンスキー 7 0 0 - 3、ユーザー ID 7 0 - 1、を、CD-RW 1 0 0 0 内の認証キー情報 9 0 に、ユーザー ID 9 0 - 1、ライセンスキー 9 0 - 3、としてアプリケーションソフトウェア名 9 0 - 2 と合わせて登録する（ステップ S 0 3 0）。さらに、当該アプリケーションソフトウェア名 9 0 - 2 に対応したアプリケーションソフトウェア 5 0 A の利用を許可して（ステップ S 0 3 1）、CD-RW 1 0 0 0 から起動する（ステップ S 0 3 2）。

【 0 0 7 7 】

ユーザーは起動されたアプリケーションソフトウェア 5 0 A を用いて、たとえば、インターネット 4 0 0 0 を経由して、各サービスの提供元の図示しない Web サーバーにアクセスして、所望のサービス提供を受ける（ステップ S 0 3 3 ）。

【 0 0 7 8 】

このように本実施の形態 2 によれば、上述の実施の形態 1 と同様の効果が得られるとともに、認証サーバー 3 0 0 0 側のアプリケーション利用情報 7 0 0 のライセンスキー 7 0 0 - 3 の設定により、個々のユーザーおよびアプリケーションソフトウェア 5 0 A 毎に多様な利用レベルを設定することが可能になる。

【 0 0 7 9 】

また、認証サーバー 3 0 0 0 の側にログ情報 6 0 0 が残るので、個々のユーザーに所有されている CD - RW 1 0 0 0 の不正使用の解析やセキュリティ管理をよりの確に行うことが可能となる。

【 0 0 8 0 】

以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【 0 0 8 1 】

たとえば、個人識別情報としては、指紋に限らず、声紋、容貌、網膜パターン、筆圧、筆跡等、高いレベルで個人識別が可能な情報を用いることができる。

【 0 0 8 2 】

また、可搬性記録媒体としては、CD - RW に限らず、MO、DVD、等の可搬性記録媒体、さらには、不揮発性の半導体メモリ等でもよい。

【 0 0 8 3 】

【 発明の効果 】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【 0 0 8 4 】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【 0 0 8 5 】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用が可能になる、という効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図である。

【図 2】

本発明の一実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図 3】

本発明の一実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図 4】

本発明の他の実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図 5】

本発明の他の実施の形態である可搬性記録媒体の使用方法にて用いられる認証サーバーの構成の一例を示す概念図である。

【図 6】

本発明の一実施の形態である可搬性記録媒体の利用方法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【符号の説明】

- 1 0 ユーザー認証プログラム
 - 1 0 - 1 ユーザー I D 管理機能
 - 1 0 - 2 指紋情報管理機能
 - 1 0 - 3 認証要求機能
- 2 0 指紋認証エンジン
 - 2 0 - 1 指紋データ抽出機能
 - 2 0 - 2 指紋照合機能
- 3 0 2 フェーズ認証プログラム
 - 3 0 - 1 認証サーバー連携機能
- 4 0 トレーサー
 - 4 0 - 1 指紋データ収集機能
- 5 0 アプリケーション管理プログラム
 - 5 0 - 1 アプリケーションライセンスキー管理機能
 - 5 0 A アプリケーションソフトウェア
- 6 0 ユーザー情報
 - 6 0 - 1 ユーザー I D
 - 6 0 - 2 指紋登録有無フラグ
- 7 0 指紋情報
 - 7 0 - 1 ユーザー I D
 - 7 0 - 2 指紋データ
- 8 0 ログ情報
 - 8 0 - 1 ユーザー I D
 - 8 0 - 2 指紋データ
- 9 0 認証キー情報
 - 9 0 - 1 ユーザー I D
 - 9 0 - 2 アプリケーションソフトウェア名
 - 9 0 - 3 ライセンスキー
- 1 0 0 ユーザー認証プログラム
 - 1 0 0 - 1 ユーザー I D 管理機能

- 2 0 0 指紋認証エンジン
- 2 0 0 - 1 指紋照合機能
- 3 0 0 トレーサー
- 3 0 0 - 1 指紋データ収集機能
- 4 0 0 アプリケーション利用管理プログラム
- 4 0 0 - 1 アプリケーション利用可否判定機能
- 4 0 0 - 2 アプリケーション利用ライセンスキー発行管理機能
- 5 0 0 ユーザー情報
- 5 0 0 - 1 ユーザー I D
- 6 0 0 ログ情報
- 6 0 0 - 1 ユーザー I D
- 6 0 0 - 2 指紋データ
- 7 0 0 アプリケーション利用情報
- 7 0 0 - 1 ユーザー I D
- 7 0 0 - 2 アプリケーションソフトウェア名
- 7 0 0 - 3 ライセンスキー
- 1 0 0 0 C D - R W
- 1 0 0 1 物理アクセスプロテクトエリア
- 1 0 0 2 リライタブルエリア
- 1 0 0 2 - 1 プロテクトエリア
- 1 0 0 2 - 2 フリーエリア
- 2 0 0 0 パーソナルコンピュータ
- 2 0 0 1 マイクロプロセッサ
- 2 0 0 2 主記憶
- 2 0 0 2 a 汎用オペレーティングシステム
- 2 0 0 3 外部記憶装置
- 2 0 0 4 可搬媒体ドライブ
- 2 0 0 5 ネットワークインタフェース
- 2 0 0 6 ユーザーインタフェース

2 0 0 7 個人識別情報入力装置

2 0 0 8 バス

3 0 0 0 認証サーバー

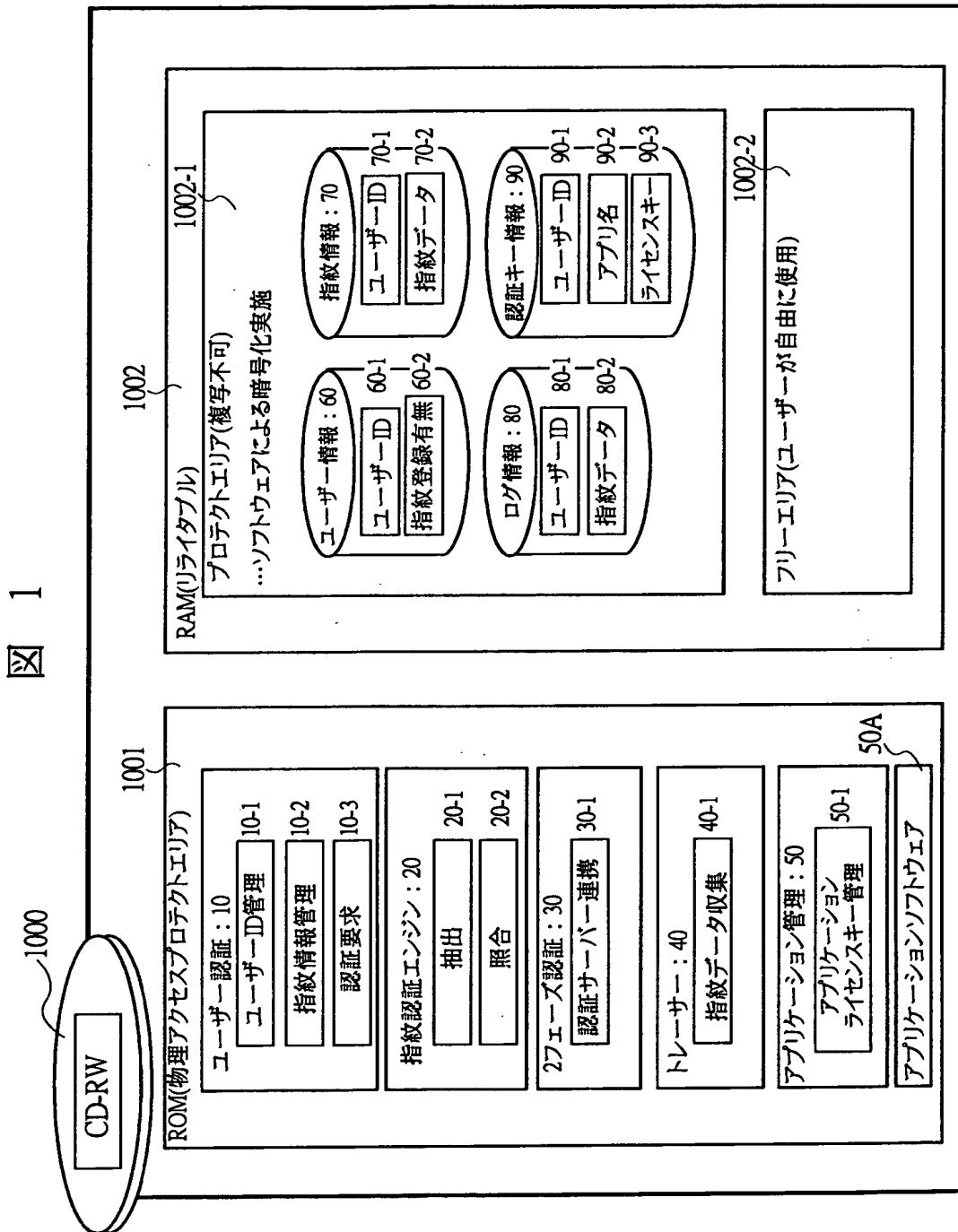
3 0 0 1 制御ソフトウェア

3 0 0 2 データベース

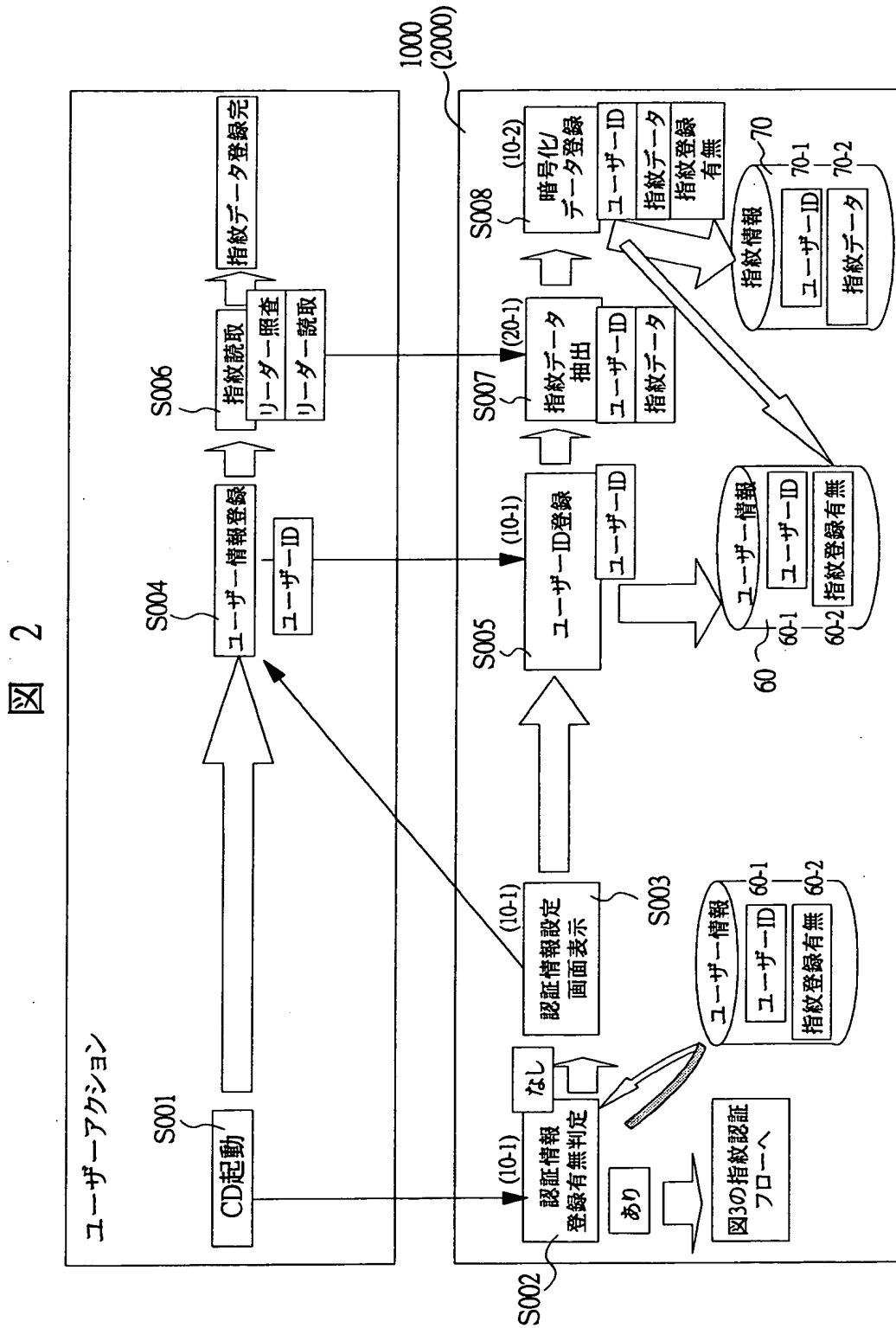
4 0 0 0 インターネット

【書類名】 図面

【図 1】

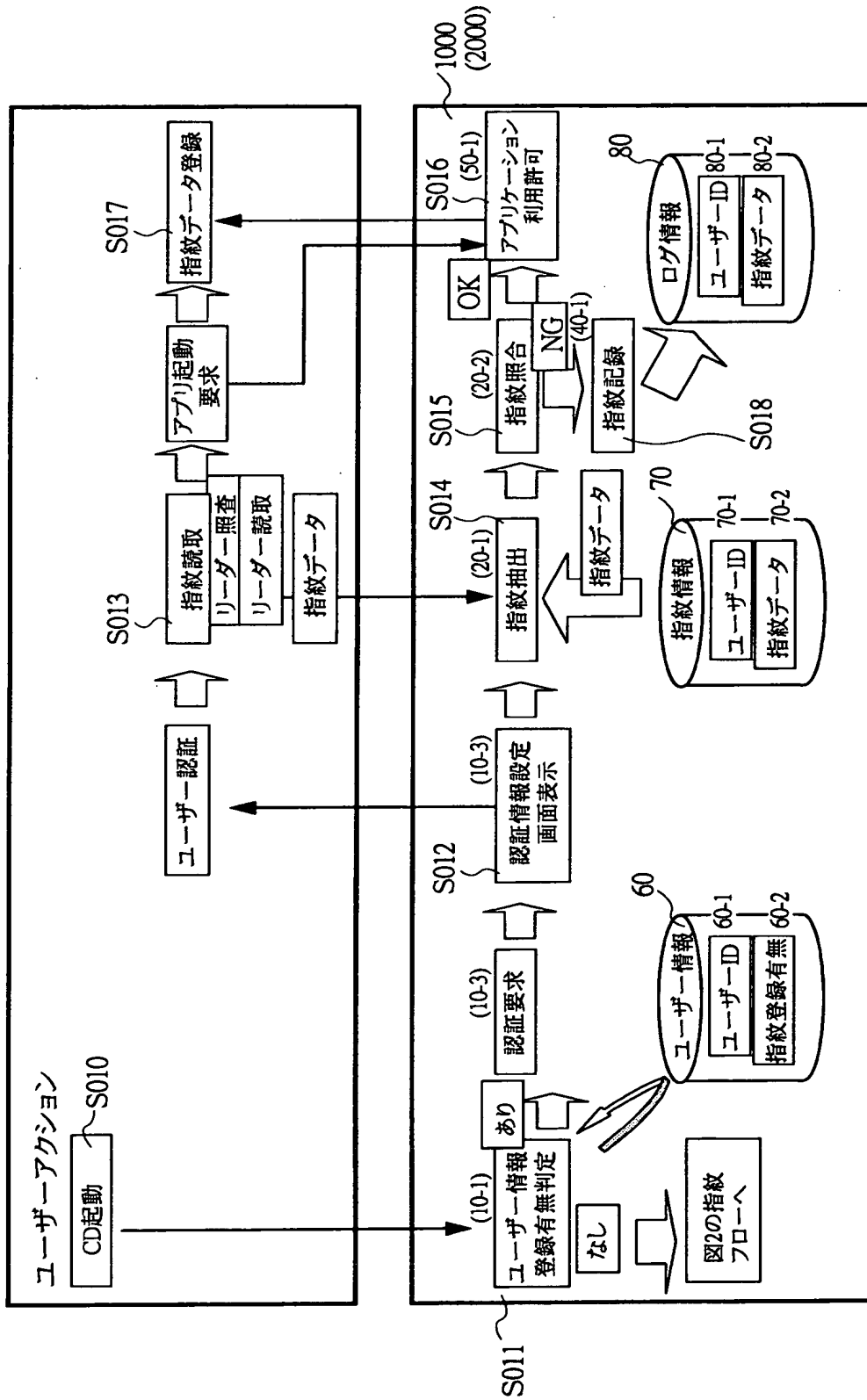


【図2】



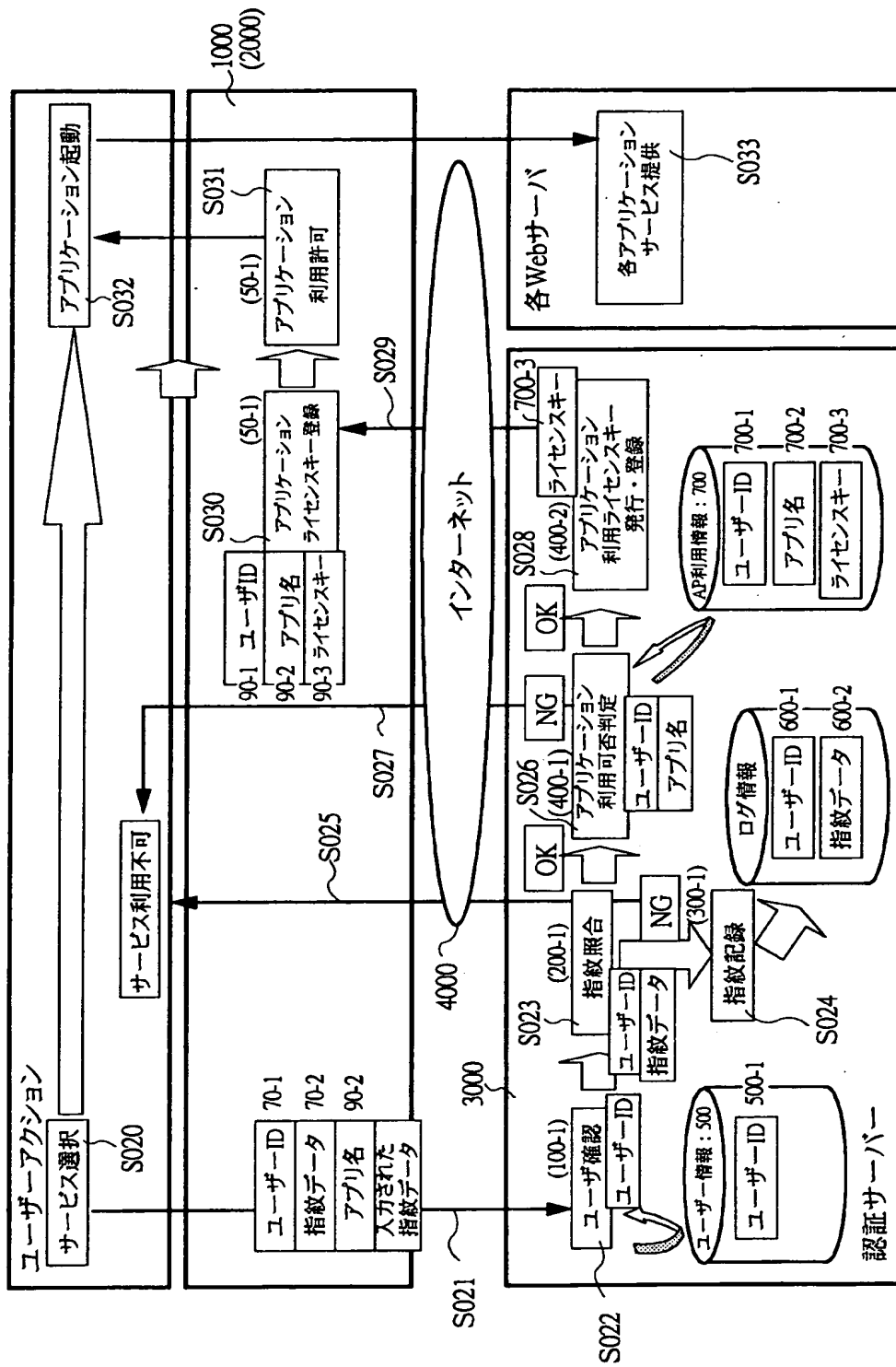
【図 3】

図 3



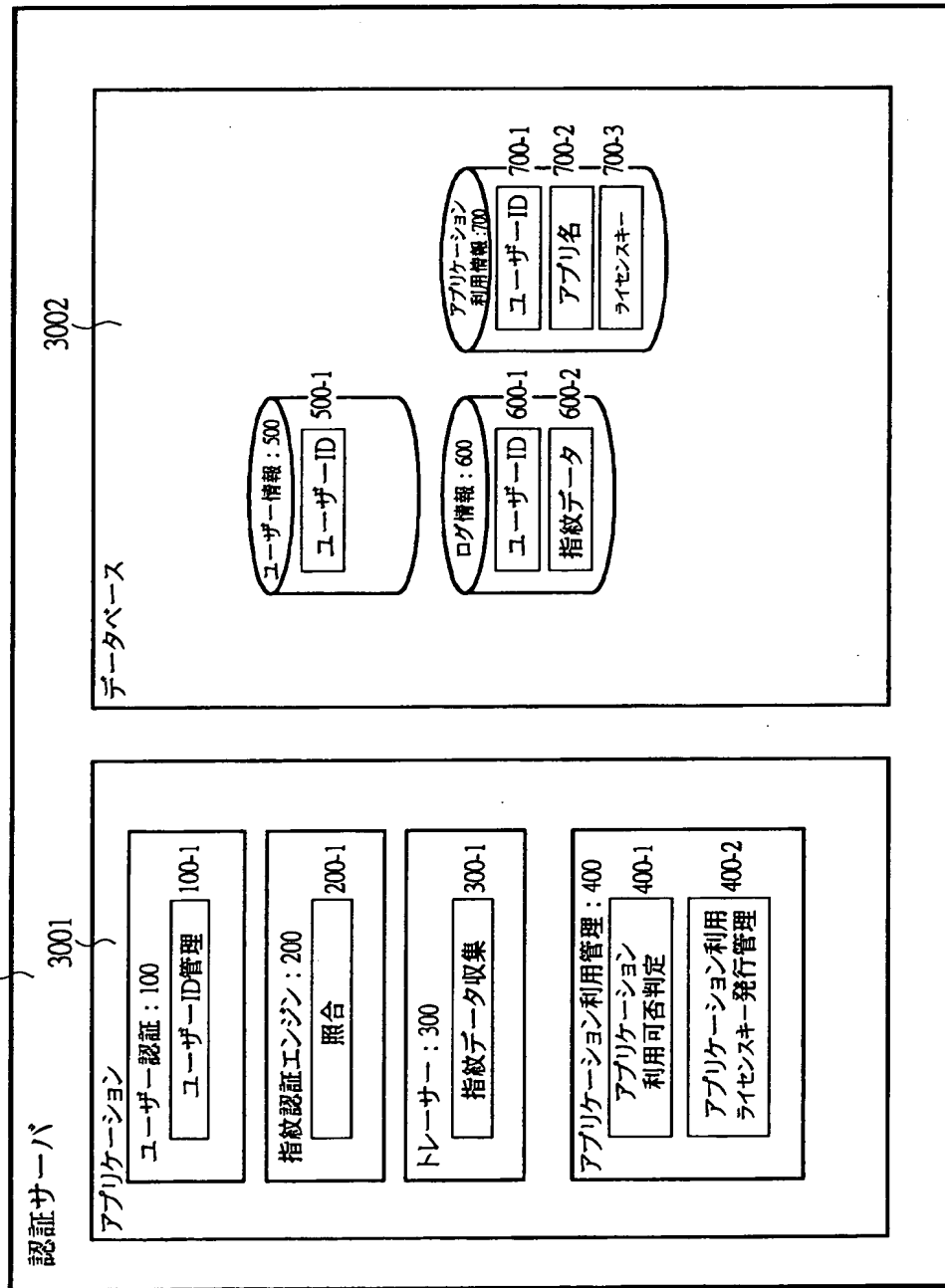
【図 4】

図 4



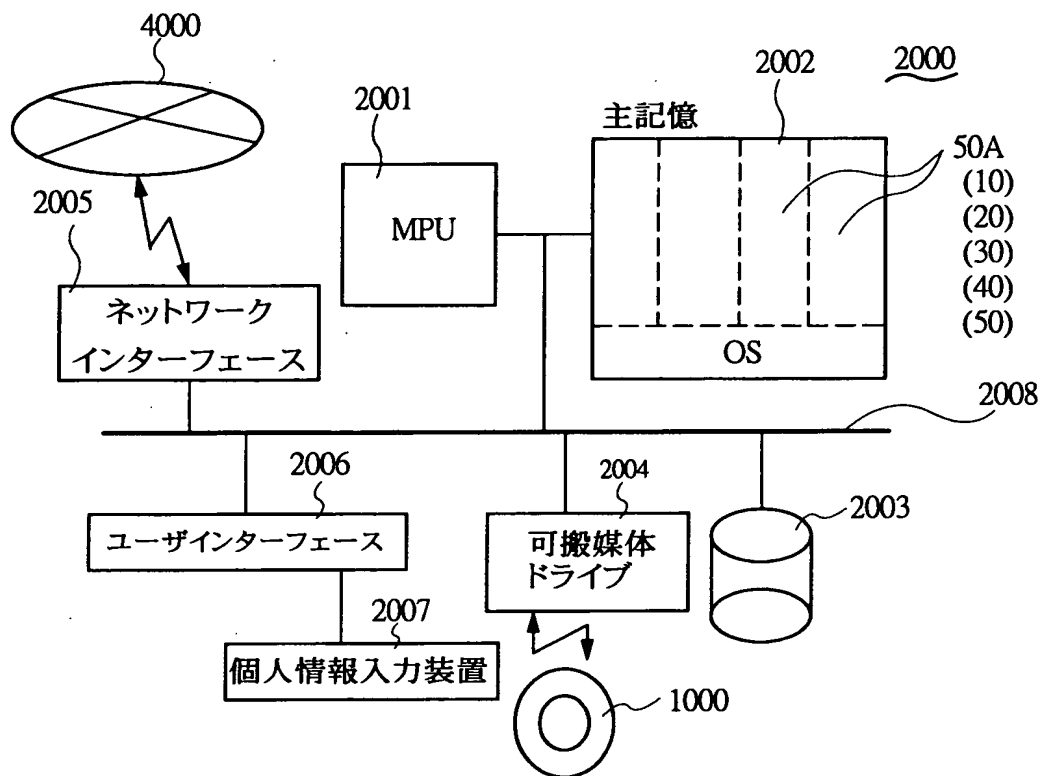
【図 5】

図 5



【図 6】

図 6



【書類名】 要約書

【要約】

【課題】 可搬性記録媒体を用いて、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする。

【解決手段】 CD-RW1000に読み出し専用の物理アクセスプロテクトエリア1001と、書き換え可能なリライタブルエリア1002を設け、物理アクセスプロテクトエリア1001には、複数のアプリケーションソフトウェア50Aと、指紋照合によるユーザー認証を行うためのユーザー認証プログラム10、指紋認証エンジン20、等を格納し、リライタブルエリア1002の複写不可のプロテクトエリア1002-1には、登録された指紋データ70-2と、対応するユーザーID70-1が格納された指紋情報70を格納し、指紋照合によるユーザー認証、および認証後のアプリケーションソフトウェア50Aの利用が、一つのCD-RW1000内で完結するようにした。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [397065952]

1. 変更年月日 1997年10月21日
[変更理由] 新規登録
住 所 東京都新宿区西新宿7-22-45
氏 名 ベーステクノロジー株式会社